ABSTRACT of the disclosure

A method of uniforming physical random numbers, capable of maintaining a random number generating rate and ensuring security concurrently. The method sequentially inputs a plurality of physical random numbers to a shift register to hold them there, and shifts them every time a reference pulse signal rises. Physical random numbers held in the shift register are randomly selected and output by a selector based on part of them. Accordingly, physical random numbers input to the shift register are uniformed and then output even thought they have a deviation, thereby eliminating the chance of not outputting random numbers or letting others recognize the deviation of random numbers.

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004年4月15日 (15.04.2004)

PCT

(10) 国際公開番号
WO 2004/031941 A1

(51) 国際特許分類[7]: G06F 7/58

(21) 国際出願番号: PCT/JP2003/012213

(22) 国際出願日: 2003年9月25日 (25.09.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-285168 2002年9月30日 (30.09.2002) JP
特願2003-101085 2003年4月4日 (04.04.2003) JP
特願2003-294101 2003年8月18日 (18.08.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ＦＤＫ株式会社 (FDK CORPORATION) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 Tokyo (JP).

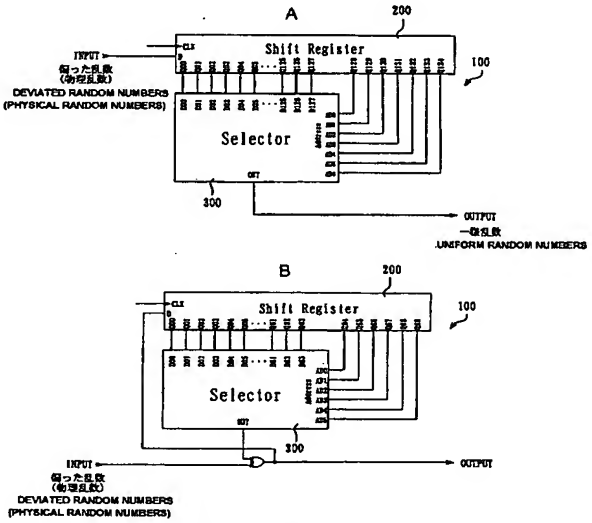
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 山本 博康 (YAMAMOTO,Hiroyasu) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). ビターナゲ アナンダ (VITHANAGE,Ananda) [LK/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 清水 隆邦 (SHIMIZU,Takakuni) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 藤田 香 (FUJITA,Kaoru) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 中野 初美 (NAKANO,Hatsumi) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 志賀 隆明 (SHIGA,Takaaki) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 曽我 竜司 (SOGA,Ryuji) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 上遠野 昌良 (KATONO,Masayoshi) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 渡邊 利幸 (WATANABE,Toshiyuki) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 鯉渕 美佐子 (KOIBUCHI,Misako) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP).

[続葉有]

(54) Title: METHOD OF UNIFORMING PHYSICAL RANDOM NUMBER AND PHYSICAL NUMBER GENERATION DEVICE

(54) 発明の名称: 物理乱数の一様化手法と物理乱数発生装置



(57) Abstract: A method of uniforming physical random numbers, capable of maintaining a random number generating velocity and ensuring security concurrently. The method sequentially inputs a plurality of physical random numbers to a shift register to hold them there, and shifts them every time a reference pulse signal rises. Physical random numbers held in the shift register are randomly selected and output by a selector based on part of them. Accordingly, physical random numbers input to the shift register are uniformed and then output even thought they have a deviation, thereby eliminating the chance of not outputting random numbers or letting others recognize the deviation of random numbers.

[続葉有]

WO 2004/031941 A1